IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

KENNETH HASSON, individually and on behalf of all others similarly situated, Plaintiff, v. COMCAST CABLE COMMUNICATIONS LLC, COMCAST CORPORATION, CITRIX SYSTEMS, INC., Defendants. This Document Relates to: All Actions	Master File No. 2:23-cv-05039-JMY The Honorable John M. Younge

COMCAST'S MEMORANDUM OF LAW IN SUPPORT OF MOTION TO STRIKE IMPROPERLY ASSERTED FACTS AND RELATED ARGUMENT FROM PLAINTIFFS' OPPOSITION TO COMCAST'S MOTIONS TO DISMISS

Pursuant to this Court's inherent authority, Defendants Comcast Cable Communications, LLC and Comcast Corporation (collectively "Comcast"), by and through undersigned counsel, hereby move to strike or, in the alternative, request that the Court disregard portions of Plaintiffs' Opposition to Defendants' Motions to Dismiss ("Opposition" to the "Motion"). (Dkt. No. 99).

I. INTRODUCTION

Plaintiffs' Opposition improperly asserts a series of new factual claims that were never included in their Complaint. These include: (1) a factually unsubstantiated assertion that "Xfinity data" was purportedly found on the dark web; (2) references to a supplemental notice letter Comcast sent to a fraction of its customers related to the Data Incident; (3) a screenshot purporting to reflect a Comcast website which Plaintiffs speculate contains the "information that Comcast uses to verify its customers"; (4) wholly improper incorporation of portions of Plaintiff Robert

Smith's Responses to Comcast's First Set of Interrogatories; and (5) an impermissible attempt to rely on speculative, unverified statements in newspaper articles to fill factual gaps in the Complaint. Plaintiffs then rely on these improperly asserted facts throughout their Opposition in an (unsuccessful) attempt to respond to and correct the deficiencies proven by Comcast's Motion.

Plaintiffs' attempt to present these new facts to the Court for consideration on a motion to dismiss is not permissible or appropriate. It is beyond dispute in this Circuit that a plaintiff cannot use new facts raised in an opposition to a motion to dismiss to cure pleading deficiencies. Yet the information that Plaintiffs belatedly and improperly seek to inject into this case, even if considered, nevertheless fails to cure the multiple, independently-fatal flaws in their Complaint. Accordingly, this Court should strike or, in the alternative, disregard these new facts and any argument premised upon them from Plaintiffs' Opposition[1] under its inherent authority without hesitation.

II. LEGAL STANDARD

"District courts . . . retain their inherent authority to control their docket," including the power to "strike from the record an improperly filed document." *Karlo v. Pittsburgh Glass Works, LLC*, No. 2:10-cv-1283, 2015 WL 3966434, at *3 (W.D. Pa. June 8, 2015). Courts routinely exercise that authority to strike or disregard filings that fail to comply with applicable rules, *see Kibbie v. BP/Citibank*, No. 3:08-cv-1804, 2009 WL 2950365, at *8 (M.D. Pa. Sept. 9, 2009), including failing to comply with the well-established rule that "courts generally may not consider matters extraneous to the pleadings" in deciding a motion to dismiss. *AT&T Corp. v. CPB Int'l, Inc.*, No. 4:05-cv-424, 2006 WL 8448277, at *5 (M.D. Pa. 2006); *see also Delaney v. Am. Express Co.*, No. 06-cv-5134, 2007 WL 9797486, at *1 (D.N.J. Feb. 8, 2007).

[1] **Exhibit A** contains a highlighted copy of Plaintiffs' Opposition demonstrating how Plaintiffs used these improperly asserted facts to support their Opposition.

III. ARGUMENT

Plaintiffs attempt to use their Opposition to improperly supplement their deficient Complaint. Yet, "[i]t is axiomatic that [a] complaint may not be amended by the briefs in opposition to a motion to dismiss." *Javaid v. Weiss*, No. 4:11-cv-1084, 2011 WL 6339838, at *6 (M.D. Pa. Dec. 19, 2011). This rule exists to ensure that "courts generally may not consider matters extraneous to the pleadings" in deciding a motion to dismiss. *AT&T Corp.*, 2006 WL 8448277, at *5. Accordingly, where, as here, a plaintiff improperly uses its opposition brief to insert facts that were not included in its complaint, courts in this Circuit have repeatedly stricken or disregarded such assertions. *See Miller v. Osauski*, No. 3:23-cv-1165, 2024 WL 3498354, at *4 (M.D. Pa. July 22, 2024) ("[T]o the extent Miller has attempted to amend his complaint by alleging additional facts in briefs opposing the motions to dismiss, these additional allegations are not considered as part of the dismissal analysis."); *Morgan v. Valley Forge Military Academy & College*, No. 21-cv-3460, 2022 WL 3229322, at *4 n.3 (E.D. Pa. Aug. 10, 2022); *SEPTA v. Orrstown Fin. Servs., Inc.*, No. 1:12-cv-993, 2016 WL 7117455, at *7 (M.D. Pa. Dec. 7, 2016); *see also Heng v. Heavner, Beyers & Mihlar, LLC*, 849 F.3d 348, 354 (7th Cir. 2017) (affirming grant of "motion to strike an exhibit that was included in appellants' response to appellee's motion to dismiss the amended complaint" because "the exhibit was not material to the complaint"); *In re Chicago Bd. Options Exchange Volatility Index Manipulation Antitrust Litig.*, 435 F. Supp. 3d 845, 872 (N.D. Ill. 2020); *Puma v. Hall*, No. 1:08-cv-1451, 2009 WL 5068629, at *5 n.3 (S.D. Ind. Dec. 17, 2009) (granting motion to strike exhibits to opposition brief because they "represent an impermissible attempt to demonstrate the reasonableness of the inferences that the Plaintiffs' argue can be drawn from their Complaint").

This Court should do the same: Because each of the five new facts Plaintiffs assert in their Opposition is an improper attempt to amend the Complaint "by the briefs in opposition to a motion to dismiss," *Javaid*, 2011 WL 6339838, at *6, they should be stricken or, at a minimum, disregarded in deciding Comcast's Motion.

A. Plaintiffs' New Assertions About a Dark Web "Search" Should Be Stricken.

Comcast's Motion demonstrated that Plaintiffs lack standing, in part, because there are no plausible allegations that Plaintiffs' information is now or ever was available on the dark web, much less because of the Data Incident. (Mot. at 9). Plaintiffs only assert "on information and belief" that their information is available on the dark web. (Compl. ¶ 297). Plaintiffs concede in Opposition that they alleged this fact on "information and belief" and that such allegations are permissible only "when the facts at issue are peculiarly within the defendant's possession." (Opp. at 29 (quoting *Lincoln Ben. Life Co. v. AEI Life, LLC*, 800 F.3d 99, 107 n. 31 (3d Cir. 2015))). But whether information from the Data Incident is circulating on the "dark web" is not a fact "peculiarly within" Comcast's possession—it is equally accessible to Plaintiffs and their counsel. Under Plaintiffs' own conceded standard, the allegation of publication is improperly pleaded and must be disregarded. *See McDermott v. Clondalkin Grp., Inc.*, 649 F. App'x 263, 268 (3d Cir. 2016); *Jason Zerbe v. Ima Financial Group, Inc.*, No. 2:24-cv-2026, 2024 WL 3677395, at *6 (D. Kan. Aug. 6, 2024) (observing that "dark web" allegations pleaded on "information and belief" are "conclusory" and "not sufficient to establish standing").

In an attempt to cure this defect, in a footnote to their Opposition and for the first time, Plaintiffs state that "[a] search on the hacking forum 'Niflheim World' revealed multiple locations where Xfinity data is being actively sold on the Dark Web," including that "accounts associated with Xfinity.com were uploaded to 'BlackBet'" in July and September 2024 and that "customer

PII associated with 'Xfinity.com'" was uploaded by someone named "BANDAI" "for sale on the Fox Store site." (Opp. at 7). None of these facts were pled in the Complaint. That alone is sufficient to strike them. But in addition, Plaintiffs include no facts supporting the veracity or credibility of these assertions. They do not identify who conducted the search, how it was conducted, nor do Plaintiffs provide any declaration or affidavit regarding the search.

Moreover, this improper, belated assertion has nothing to do with *Plaintiffs*. The screen shot that Plaintiffs reference in Footnote 2 of their Opposition does not include any information about Plaintiffs.[2] Comcast has tens of millions of customers; even if the 175 Xfinity credentials supposedly offered for sale were authentic, nothing but wild speculation—which this Court cannot entertain—supports the conclusion that these 175 Xfinity credentials relate to any of these named Plaintiffs. *UPMC Pinnacle v. Shapiro*, 377 F. Supp. 3d 449, 455 (M.D. Pa. 2019) (holding that court is "not required to credit mere speculation" at the motion-to-dismiss stage). Nor is there more that would tie the 175 Xfinity credentials to the Citrix Bleed vulnerability and not some other source, such as a compromise of user devices, phishing scams, credential stuffing, and the use of malware, that have nothing to do with the exploitation of a vulnerability such as Citrix Bleed.[3] Indeed, it seems unlikely that a rational threat actor would steal 36 million hashed credentials yet try to sell them off 175 at a time.

---

[2] **Exhibit B** contains the screenshot, provided to Comcast in Plaintiffs' response to Comcast's First Request for Production. Because Plaintiffs marked this screenshot as Confidential pursuant to the Protective Order, it has been filed preliminarily under seal.

[3] Flare Systems, Inc., *Dark Web Leaks: Stolen Credentials on the Dark Web*, https://flare.io/learn/resources/blog/dark-web-leaks/ ("Phishing attacks are deceptive tactics that trick users into revealing their credentials . . . . Certain types of malware, such as keyloggers or spyware, can record keystrokes, capture screenshots, and monitor user activity to gather sensitive information, which can then be sent to the cybercriminal . . . . In credential stuffing attacks, cybercriminals use automated tools to test combinations of usernames and passwords across multiple website."); NIST, *Computer Security Resources Center*, CSRC.NIST.GOV, https://csrc.nist.gov/glossary/term/key_logger.

In short, there is simply no basis to believe that Plaintiffs' new assertions regarding Xfinity information on the Dark Web have anything to do with the Data Incident. These belated facts are not simply late, but lack any foundation that could authenticate them or their relevance. But the Court certainly need not decide, at this posture, where these supposed credentials come from, whether they are legitimate, or any other factual matter. Comcast only asks that the Court reject this out-of-time effort to cure the Complaint's deficiencies in considering the Motion. Footnote 2 and all references to it and arguments made based on it in Plaintiffs' Opposition should be stricken.

B. Plaintiffs' New Assertions About the Supplemental Letter Should be Stricken.

Plaintiffs' Complaint does not allege that any of *their* sensitive information, such as full Social Security numbers, was compromised in the attack on Comcast. Rather, Plaintiffs merely cite to the breach notification letter from December 2023 that informed these Plaintiffs that, e.g., the last four digits of their Social Security numbers may have been compromised. (Compl. ¶ 11). This is the notification that was sent to almost 36 million persons, including the named Plaintiffs, and which is relied upon in the Complaint.[4]

The last four digits of a Social Security number is not sensitive information. Indeed, as set forth in the Motion to Dismiss, the last four digits of a Social Security number are routinely allowed to be posted on public dockets under both federal and state laws. (Mot. at 11–12). Therefore, the compromise of the last four digits of a Social Security number does not represent an Article III injury and does not constitute actual damage. *See, e.g., Scifo v. Alvaria, Inc.*, No. 23-cv-10999-ADB, 2024 WL 4252694, *1 (D. Mass. Sept. 20, 2024) (finding no standing for data breach of last four digits of Social Security number coupled with personal and loan information).

[4] Maine Attorney General, *Data Breach Notifications*, MAINE.GOV (Dec. 18, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml.

Plaintiffs seem to anticipate losing this argument, and they should. In their Opposition, Plaintiffs therefore belatedly note that Comcast sent a supplemental letter "for a portion of its customers" on January 26, 2024. (Opp. at 7). For those customers, the breach involved full Social Security numbers and/or driver's license numbers. Comcast issued the January 2024 supplemental notice more than five months before Plaintiffs filed the operative Complaint, yet Plaintiffs failed to include any assertions related to the Supplemental Letter in their Complaint.

To be sure, even if Plaintiffs *had* referenced the supplemental notice in the Complaint, that would not change anything: The Supplemental Notice was sent to 2,302 persons out of Comcast's tens of millions of customers,[5] yet not a single named Plaintiff alleges that *they* received the Supplemental Notice. They did not, because none of them had full Social Security numbers or driver's license numbers compromised. But regardless, Plaintiffs' effort after the fact to find some new support for the assertion of their Social Security number claims at this late date should not be countenanced. Facts and argument related to the Supplemental Notice should be stricken from Plaintiffs' Opposition.

C. Plaintiffs' New Facts About Xfinity's Authentication Process Should Be Stricken.

As explained in Comcast's Motion, none of the types of information identified in the December 2023 Notice Letter that these Plaintiffs actually received could be used to commit identity theft or financial fraud. (Mot. at 20–21). Absent this connection, Plaintiffs cannot establish a substantial future risk of identity theft. *See, e.g.*, *In re VTech Data Breach Litig.*, No. 15-cv-10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) ("[P]laintiffs do not explain how the stolen data would be used to perpetrate identity theft."); *In re Uber Techs., Inc., Data Sec.*

[5] Maine Attorney General, *Data Breach Notifications*, MAINE.GOV (Jan. 26, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/202cb122-b4e6-42fd-b9b5-59e59d44d4fe.shtml.

Breach Litig., No. 18-cv-2970, 2019 WL 6522843, at *6 (C.D. Cal. Aug. 19, 2019) ("[I]t is not apparent to the Court how the disclosure of Plaintiff's basic contact information and driver's license number could be plausibly used to gain access to his tax return or make fraudulent charges on his credit and debit cards."). Those Plaintiffs who do assert actual or attempted identity misuse do not allege facts plausibly tracing such misuse to the Data Incident. *See, e.g., Burger v. Healthcare Mgmt. Sols*., LLC, No. 23-cv-1215, 2024 WL 473735, at *6 (D. Md. Feb. 7, 2024) (dismissing data breach class action under Rule 12(b)(1) where plaintiff's alleged instances of data misuse could not be "fairly traced" to either defendant).

Sensitive to this failing, in their Opposition, Plaintiffs assert that the information at issue in the Data Incident is "the same information that Comcast uses to verify its customers" and includes a screenshot of what appears to be a Comcast webpage. (Opp. at 14). Neither this screenshot nor anything about what "information . . . Comcast uses to verify its customers" were alleged in the Complaint. Plaintiffs provide no web address (url) identifying where they obtained the screenshot. Plaintiffs provide no declaration or affidavit. Plaintiffs do not even attempt to explain when this form would be displayed, or what happens when the form is submitted. Plaintiffs failed to provide even a single indicia of credibility or authentication related to the screenshot. Plaintiffs simply imply that this information would be sufficient to access an Xfinity account.

Should this matter proceed further into discovery, Comcast will prove that the information described in the Complaint, using the process Plaintiffs identified, would *not* allow access to any Xfinity account. But Comcast does not ask the Court, at this juncture, to decide that factual dispute. Comcast only asks that this belated factual assertion and screenshot, both absent from the Complaint, and any argument premised upon them be stricken from Plaintiffs' Opposition and disregarded when deciding the Motion to Dismiss.

D. Plaintiffs' New Assertions About Smith's Discovery Responses Should be Stricken.

Plaintiffs' claim under § 551(e) of the Cable Act should be dismissed, among other reasons, because not one Plaintiff alleges that they are a former Comcast subscriber whose information was retained beyond the "purpose for which it was collected," or that any supposed "over retention" was the cause of any concrete or imminent injury. (Mot. at 25–26). Apparently realizing that their Section 551(e) "over retention" claim is fatally deficient, Plaintiffs' Opposition now asserts that Plaintiff Smith has standing under Section 551(e) because he is a former customer. (Opp. at 33).

To support this new assertion—which, like all others addressed herein, is nowhere in the Complaint—Plaintiffs attach a portion of Smith's Response to Comcast's First Set of Interrogatories to their Opposition. (*Id.* at 33 n.18). It is beyond dispute that it is wholly inappropriate to attach an interrogatory response to oppose a motion to dismiss and to attempt to cure deficiencies in the complaint. *See Miller v. Osauski*, No. 3:23-cv-1165, 2024 WL 3498354, at *4 (M.D. Pa. July 22, 2024); *Morgan v. Valley Forge Military Academy & College*, No. 21-cv-3460, 2022 WL 3229322, at *4 n.3 (E.D. Pa. Aug. 10, 2022) ("[T]o the extent Miller has attempted to amend his complaint by alleging additional facts in briefs opposing the motions to dismiss, these additional allegations are not considered as part of the dismissal analysis."); *SEPTA v. Orrstown Fin. Servs., Inc.*, No. 1:12-cv-993, 2016 WL 7117455, at *7 (M.D. Pa. Dec. 7, 2016). As a matter of black letter law, this Court cannot consider this self-serving, factual assertion. *See Mackenzie v. Hutchens*, No. 12-cv-584, 2013 WL 8291423, at *12 (C.D. Cal. Sept. 9, 2013) (explaining that the "court cannot consider material outside the complaint," including "*facts presented in briefs, affidavits or discovery materials*").

If Plaintiffs wanted to assert such a fact, they should have conducted reasonable diligence in speaking with Plaintiff Smith *in advance* of filing their Consolidated Complaint in July 2024.

Or they could have exercised their ability to amend the Complaint further as a matter of right under Rule 15(a)(1)(B). Plaintiffs did neither. Plaintiffs should not, and as a matter of law cannot, be permitted to amend their Complaint via their Opposition to Comcast's Motion to Dismiss. Should this case persist into discovery, Comcast will prove that Plaintiff Smith's contentions are incorrect as a matter of fact and a matter of law. But for now, the Court should strike Plaintiff Smith's interrogatory answer and any argument premised upon it or, at a minimum, refuse to consider any facts contained therein which were not properly pled.

E. Plaintiffs' Reference to Unalleged Statements in News Articles Should Be Stricken.

The Complaint fails to identify the third party that attacked Comcast, and moreover fails to allege that third party's motive. For example, the Complaint never alleges that the Data Incident was part of a ransomware scheme, nor that Comcast received a ransom demand. As explained in Comcast's Motion, (Mot. at 15), these failures undermine any suggestion of an "imminent" or "substantial risk" of identity theft. Aware of this fatal defect, the Opposition newly inserts the characterization of the threat actor as a "ransomware gang". No factual allegation in the Complaint would support such a characterization. Instead, the Opposition refers to a news article cited in Footnote 87 of the Complaint. Plaintiffs cite to that news article for the proposition that an unidentified "[r]ansomware gang" was "likely" behind the Data Incident. (Opp. at 18). But the Complaint does not rely on or quote the article for this speculative proposition. Plaintiffs cannot evade their obligations under Rules 8 and 11 by cherry-picking from myriad news articles, briefly mentioned in footnotes, to "fill factual holes in the complaint's allegations." *Walker v. S.W.I.F.T. SCRL*, 517 F. Supp. 2d 801, 806 (E.D. Va. 2007) ("To conclude otherwise would allow parties to circumvent Rule 11's duty to conduct 'an inquiry reasonable under the circumstances[.]'"). The Opposition's reliance on these statements from the article referred to in Footnote 87 must be

stricken or disregarded. Moreover, even if considered, that news article does not name Comcast at all, but mentions other companies, such as Boeing and the Industrial and Commercial Bank of China as having been targeted by ransomware attacks following Citrix Bleed. Only a compound chain of impermissible speculation would lead, obliquely, to the supposition that the same threat actor(s) that attacked these other, unrelated companies attacked Comcast for the same reason. References in the Opposition to a supposed ransomware gang or motive should be stricken and/or disregarded.

CONCLUSION

For the forgoing reasons, the Court should grant Comcast's Motion to Strike the improper new assertions and all argument premised upon them from Plaintiffs' Opposition brief as set forth in Exhibit A.[6]

Dated: October 30, 2024

Respectfully Submitted,

By: *Paul Bond*

Paul Bond (*admitted pro hac vice*)
Justin Kadoura (I.D. No. 324212)
HOLLAND & KNIGHT LLP
1650 Market Street, Suite 3300
Philadelphia, Pennsylvania 19103
(215) 252-9537
paul.bond@hklaw.com
justin.kadoura@hklaw.com

Mark S. Melodia (I.D. No. 53515)
Sophie L. Kletzien (*admitted pro hac vice*)
HOLLAND & KNIGHT LLP
787 Seventh Avenue, 31st Floor
New York, New York 10019
(212) 513-3583
mark.melodia@hklaw.com
sophie.kletzien@hklaw.com

[6] Leave to amend is proper only if the amendment will cure the problems with the Complaint. *Knopick v. UBS Fin. Servs., Inc.*, 121 F. Supp. 3d 444, 465 (E.D. Pa. 2015). As explained above, the improper new allegations in Plaintiffs' Opposition brief cannot do so. Accordingly, leave to amend should be denied.

Caitlin F. Saladrigas (*admitted pro hac vice*)
HOLLAND & KNIGHT LLP
777 South Flagler Drive, Suite 1900
West Palm Beach, Florida 33401
(561) 833-2000
caitlin.saladrigas@hklaw.com

William F. Farley (*admitted pro hac vice*)
Steven A. Block (*admitted pro hac vice*)
HOLLAND & KNIGHT LLP
150 North Riverside Plaza, Suite 2700
Chicago, IL 60606
(312) 578-6698
william.farley@hklaw.com
steven.block@hklaw.com

Counsel for Comcast Cable Communications LLC and Comcast Corporation